(12) UK Patent Application (19) GB (11) 2 357 225 (13) A

(43) Date of A Publication 13.08.2001

(21) Application No 9929029.8

(22) Date of Filing 08.12.1999

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto, California 94304,
United States of America

(72) Inventor(s)
Michael John Wray

(74) Agent and/or Address for Service
Robert Francis Squibbs
Hewlett-Packard Limited, Intellectual Property
Section, Building 2, Filton Road, Stoke Gifford,
BRISTOL, BS12 6QZ, United Kingdom

(51) INT CL[7]
H04L 9/32

(52) UK CL (Edition S)
H4P PDCSA

(56) Documents Cited
EP 0586022 A1 EP 0503765 A2 WO 96/02993 A2

(58) Field of Search
UK CL (Edition R) G4A AAP , H4P PDCSA
INT CL[7] G06F 1/00 , H04L 9/32
Online: EPODOC, JAPIO, WPI

(54) Abstract Title
Electronic certificate with validity subject to external conditions

(57) An electronic or digital certificate has content data specifying an attribute delegation, some benefit or right conferred by the certificate, from an identified issuer to the subject of the certificate. The content data also specifies a condition (40) that must be met for the delegation to be valid. The certificate may identify the subject who is delegated the attribute by the certificate or any subject which satisfies the condition may be delegated the attribute. The condition requires that a particular subject must have a particular attribute in order to meet the criteria for the condition, this particular subject may or may not be the same as the subject of the certificate.

The condition may specify multiple attributes that the particular subject must have which may be combined in a logical relationship.

The certificate also includes an electronic or digital signature confirming its contents and may be an SPKI certificate.

Reduction and trust chain discovery engines for use with the certificates are also disclosed.

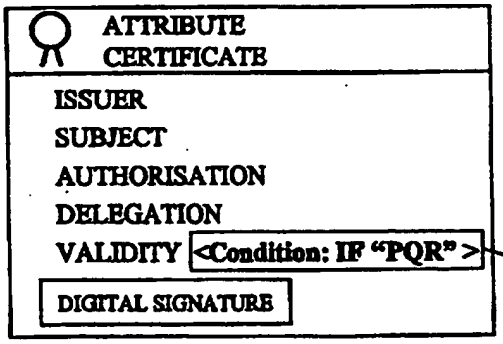


Figure 5

GB 2 357 225 A

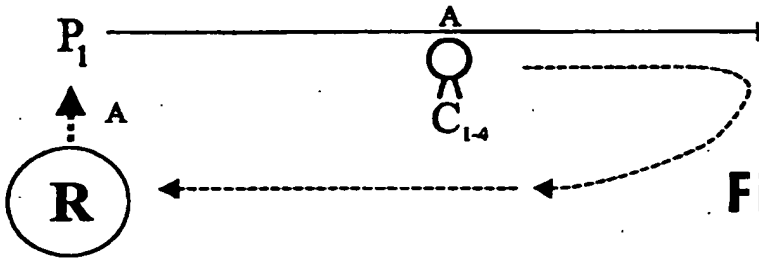


Figure 1
(PRIOR ART)

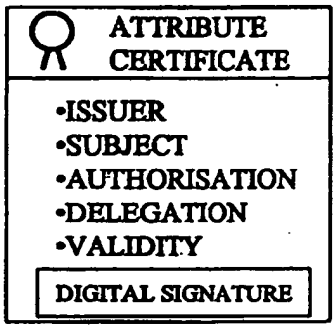
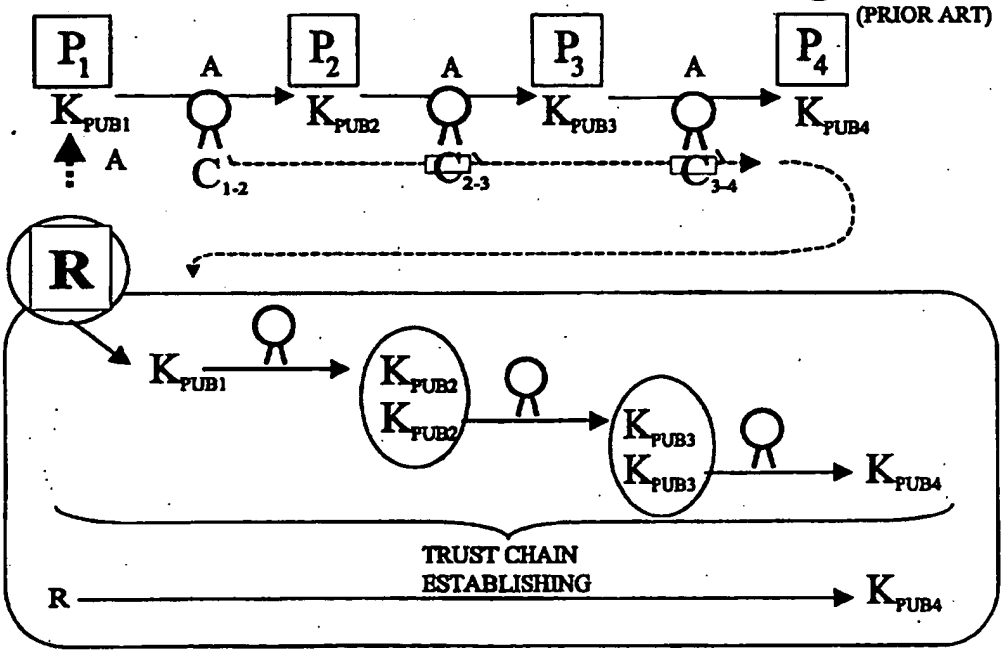


Figure 2
(PRIOR ART)

Figure 3
(PRIOR ART)



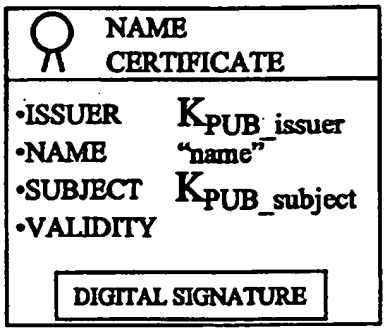


Figure 4
(PRIOR ART)

$$K_{PUB_issuer} \bullet \text{"name"} = K_{PUB_subject}$$

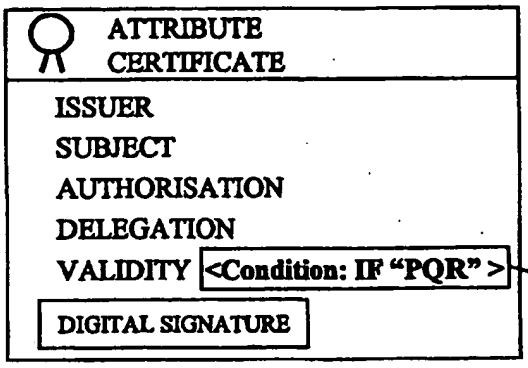
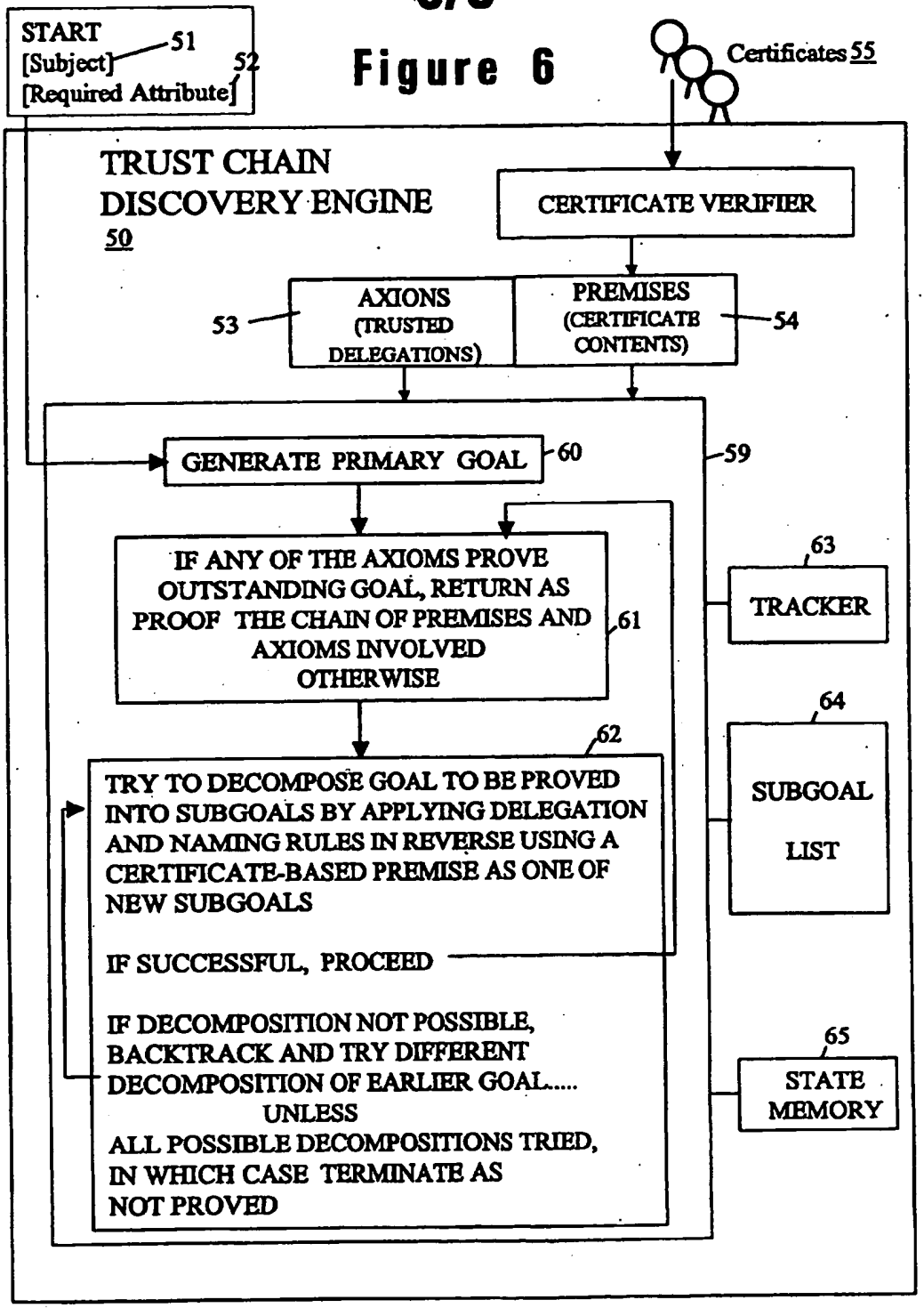


Figure 5

Figure 6


START
[Subject] 51
[Required Attribute] 52
Certificates 55
TRUST CHAIN DISCOVERY ENGINE 50
CERTIFICATE VERIFIER
53
AXIONS (TRUSTED DELEGATIONS)
PREMISES (CERTIFICATE CONTENTS)
54
GENERATE PRIMARY GOAL 60
59
IF ANY OF THE AXIOMS PROVE OUTSTANDING GOAL, RETURN AS PROOF THE CHAIN OF PREMISES AND AXIOMS INVOLVED OTHERWISE 61
63
TRACKER
64
SUBGOAL LIST
62
TRY TO DECOMPOSE GOAL TO BE PROVED INTO SUBGOALS BY APPLYING DELEGATION AND NAMING RULES IN REVERSE USING A CERTIFICATE-BASED PREMISE AS ONE OF NEW SUBGOALS
IF SUCCESSFUL, PROCEED
IF DECOMPOSITION NOT POSSIBLE, BACKTRACK AND TRY DIFFERENT DECOMPOSITION OF EARLIER GOAL.....
UNLESS
ALL POSSIBLE DECOMPOSITIONS TRIED, IN WHICH CASE TERMINATE AS NOT PROVED
65
STATE MEMORY

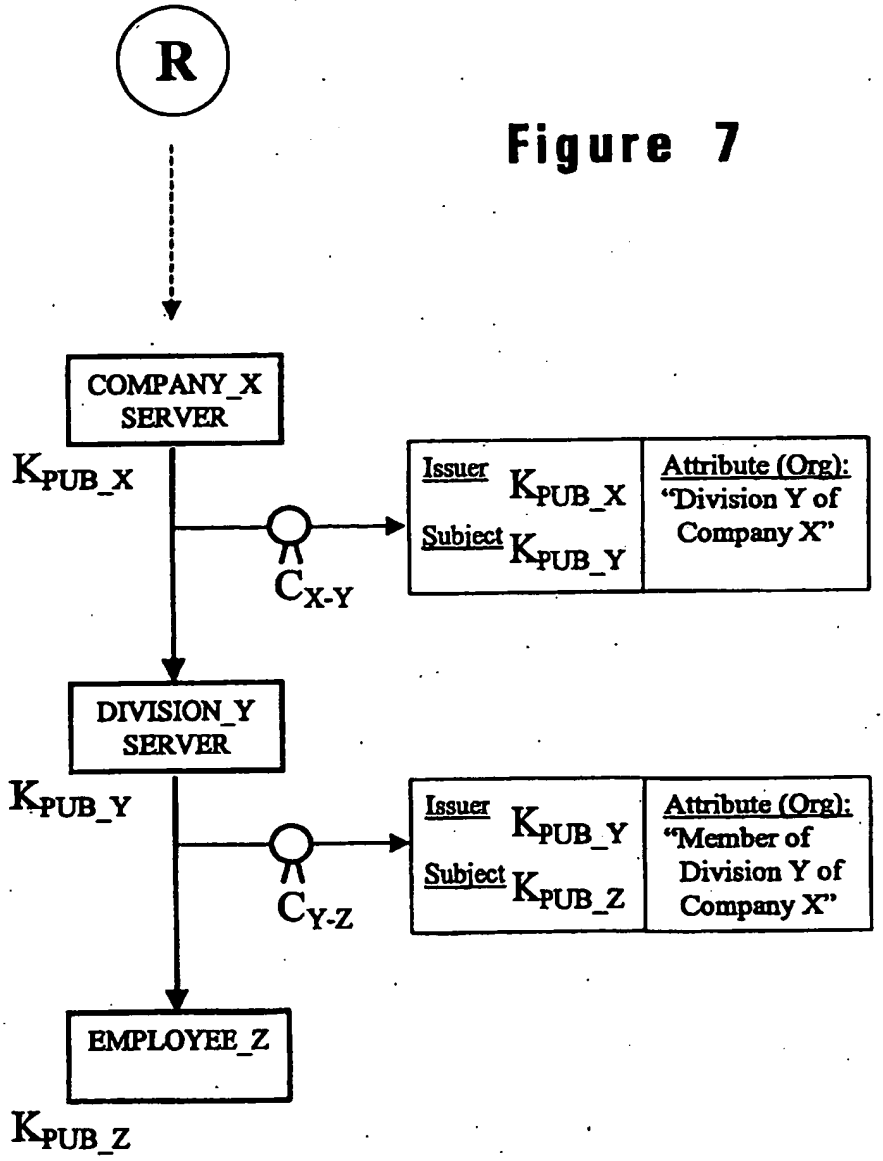

R
COMPANY_X SERVER
K_{PUB_X}
C_{X-Y}
Issuer K_{PUB_X}
Subject K_{PUB_Y}
Attribute (Org): "Division Y of Company X"
DIVISION_Y SERVER
K_{PUB_Y}
C_{Y-Z}
Issuer K_{PUB_Y}
Subject K_{PUB_Z}
Attribute (Org): "Member of Division Y of Company X"
EMPLOYEE_Z
K_{PUB_Z}

Figure 7

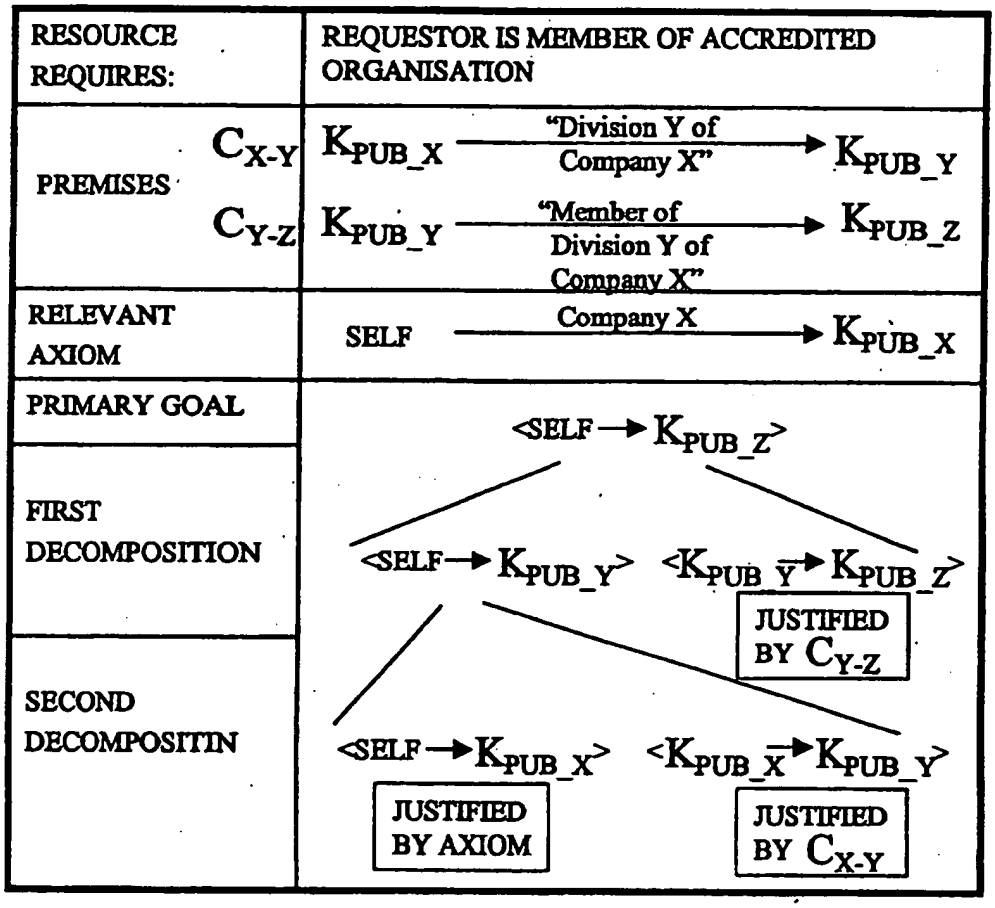

RESOURCE REQUIRES:
REQUESTOR IS MEMBER OF ACCREDITED ORGANISATION
PREMISES
C_{X-Y}
K_{PUB_X} "Division Y of Company X" K_{PUB_Y}
C_{Y-Z}
K_{PUB_Y} "Member of Division Y of Company X" K_{PUB_Z}
RELEVANT AXIOM
SELF Company X K_{PUB_X}
PRIMARY GOAL
<SELF → K_{PUB_Z}>
FIRST DECOMPOSITION
<SELF → K_{PUB_Y}>
<K_{PUB_Y} → K_{PUB_Z}>
JUSTIFIED BY C_{Y-Z}
SECOND DECOMPOSITIN
<SELF → K_{PUB_X}>
<K_{PUB_X} → K_{PUB_Y}>
JUSTIFIED BY AXIOM
JUSTIFIED BY C_{X-Y}

Figure 8

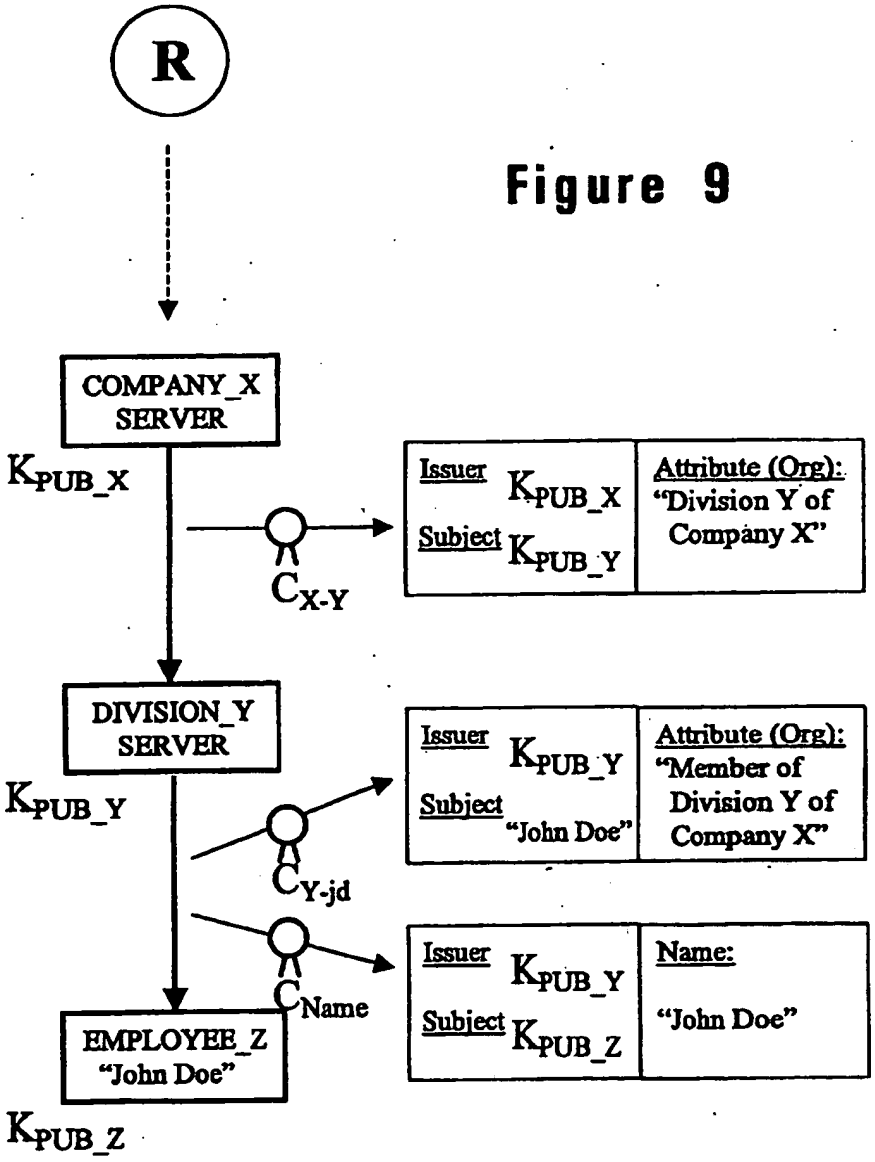

R
COMPANY_X SERVER
K_{PUB_X}
C_{X-Y}
Issuer K_{PUB_X}
Subject K_{PUB_Y}
Attribute (Org): "Division Y of Company X"
DIVISION_Y SERVER
K_{PUB_Y}
C_{Y-jd}
Issuer K_{PUB_Y}
Subject "John Doe"
Attribute (Org): "Member of Division Y of Company X"
C_{Name}
Issuer K_{PUB_Y}
Subject K_{PUB_Z}
Name: "John Doe"
EMPLOYEE_Z "John Doe"
K_{PUB_Z}

Figure 9

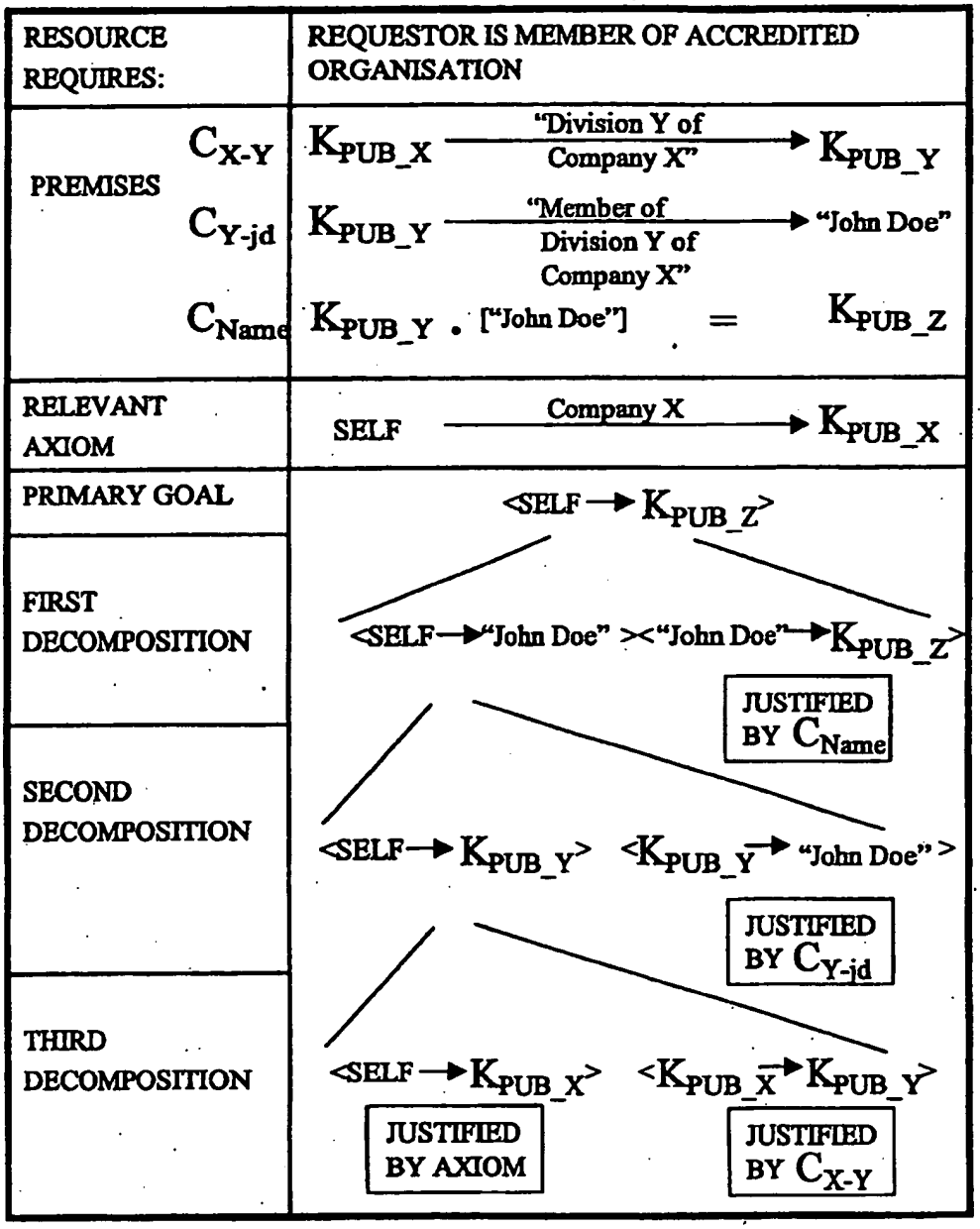

RESOURCE REQUIRES:
REQUESTOR IS MEMBER OF ACCREDITED ORGANISATION
PREMISES
C_{X-Y}
K_{PUB_X} "Division Y of Company X" K_{PUB_Y}
C_{Y-jd}
K_{PUB_Y} "Member of Division Y of Company X" "John Doe"
C_{Name}
K_{PUB_Y} . ["John Doe"] = K_{PUB_Z}
RELEVANT AXIOM
SELF Company X K_{PUB_X}
PRIMARY GOAL
<SELF → K_{PUB_Z}>
FIRST DECOMPOSITION
<SELF → "John Doe" >< "John Doe" → K_{PUB_Z}>
JUSTIFIED BY C_{Name}
SECOND DECOMPOSITION
<SELF → K_{PUB_Y}> <K_{PUB_Y} → "John Doe" >
JUSTIFIED BY C_{Y-jd}
THIRD DECOMPOSITION
<SELF → K_{PUB_X}> <K_{PUB_X} → K_{PUB_Y}>
JUSTIFIED BY AXIOM
JUSTIFIED BY C_{X-Y}

Figure 10

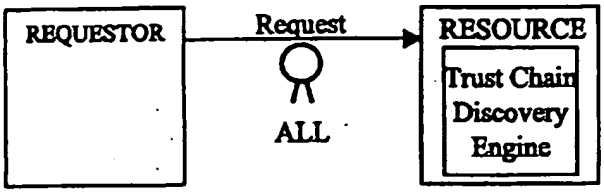


Figure 11

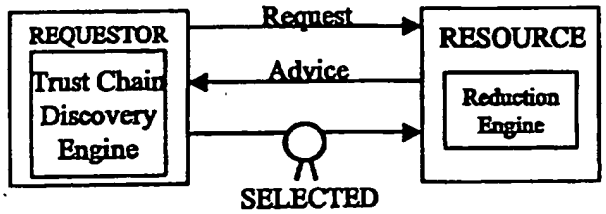


Figure 12

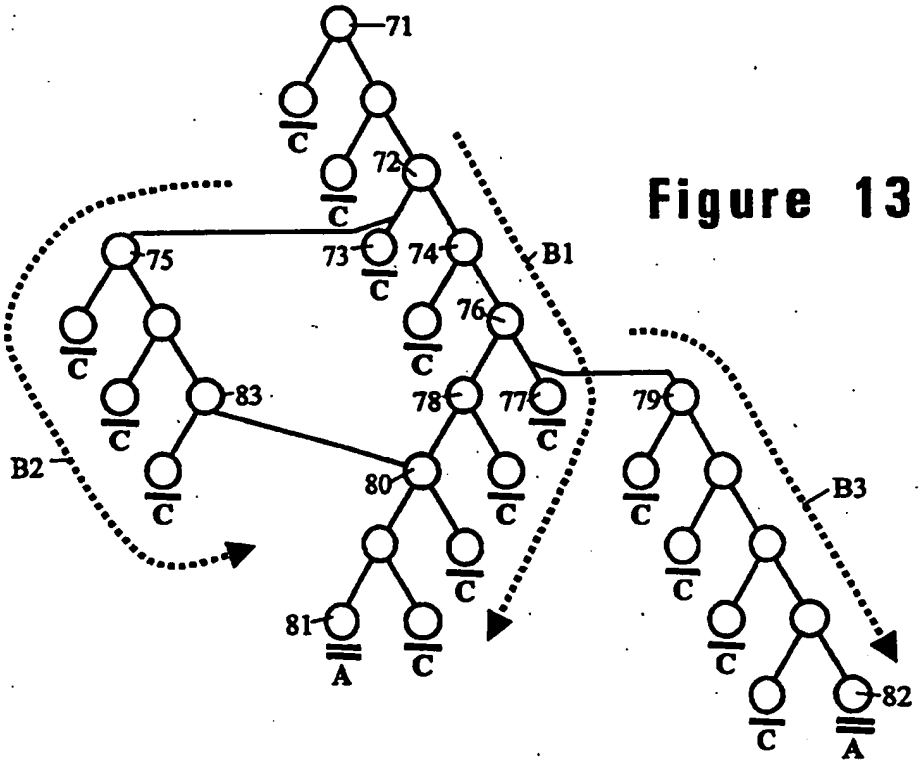


Figure 13